PI magazine .com

professional investigator magazine

$9.95

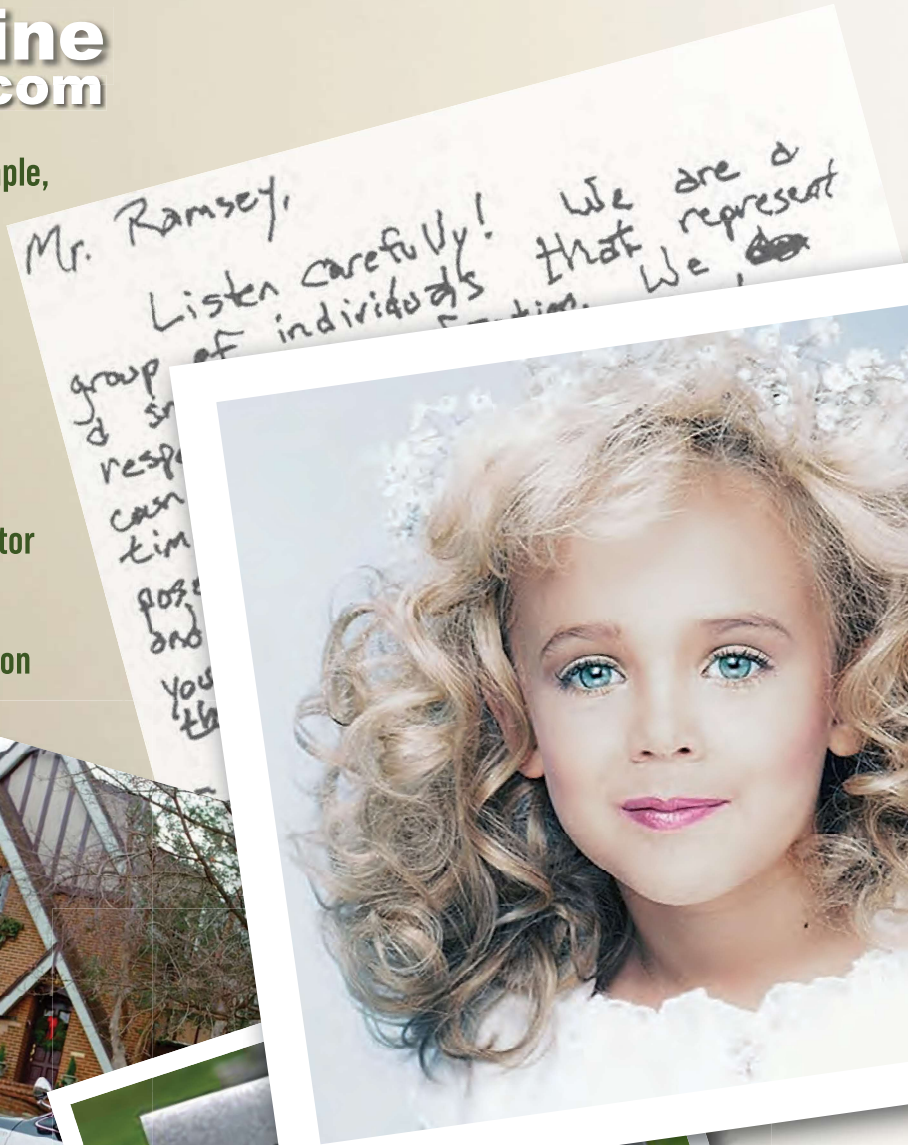
July/August 2024

THE CHECKLIST: A Simple, Yet Essential Guide

APP-SOLUTE INSIGHT Harnessing Everyday Apps for Open Source Intelligence

DEMOGRAPHICS for the Private Investigator

STOICISM and the Art of Private Investigation



CA SENATE BILL 553 Increased Business Opportunities for Security Consultants

Navigating the Depths of WRONGFUL DEATH INVESTIGATIONS

Don't Hold Back

The last of a four-part series on the JonBenét Ramsey Case

DEPARTMENTS

IN EVERY ISSUE

METADATA

It May Be Useful But It May Be Unreliable

BY **ROBERT B. FRIED**

Perhaps you want to know who authored an 850-word document on a computer? Maybe you would like to know who last modified or printed the document? Metadata is defined as data about data. It can be useful to an investigator, providing key information that may be vital to an investigation.

Electronic evidence is fragile; and therefore, must be handled with care. Engaging a data collection specialist will ensure that the targeted data is collected in a forensically sound manner, whereas the integrity of the source data, including any associated metadata, is maintained. Simply copying and pasting a document from one storage volume to another may impact its metadata – specifically file created or last access dates and times. Other ways that metadata can be modified include updating values in a document's properties via an operating system or utilizing a hex-editor.

It may be apparent by now that metadata is useful but it's not necessarily reliable. Reviewing a document's metadata alone may not reveal all the available information about a file. It's important to consider how the document was created, who interacted with it, and where it was saved (if different from its current storage location). Metadata may only provide limited information about a document's lifecycle. It's important for the forensic examiner to have as much context as possible. Therefore, a forensic examiner may recommend obtaining a forensic image of the device or storage location where

the document is stored (remember, copies of a document may be stored in multiple locations, and different versions may exist). A forensic examiner can analyze a forensic image – specifically artifacts from the operating system or file system to learn more about a document. For example, a forensic examiner may be able to determine the series of actions and the dates and times associated with a computer user saving a document into a folder C:/Robert, and then subsequently copying it into another folder, C:/Fried.

Before taking any action on electronic evidence encountered during an investigation, it's prudent to contact a data collection specialist. These individuals are trained to establish a proper chain of custody, preserve and collect evidence in a defensible and efficient manner – preventing claims of data spoilation – and ensuring its admissibility in a court of law. **PI**

Robert B. Fried has nearly 25 of experience performing data collections and forensic investigations of electronic evidence. He is the Senior Vice President and Global Head of Sandline Discovery's Forensics and Investigations practice. Prior to joining Sandline, he was a Senior Director for Consilio's Digital Forensics & Expert Services. Robert has also held senior-level positions for the data forensics practices at Huron Consulting Group and DOAR Litigation Consulting. Robert is a licensed Professional Investigator in Michigan and is a licensed Private Investigator in New York. Previously, Robert was a Computer Crime Specialist at the National White Collar Crime Center (NW3C), where he developed and instructed computer forensic and investigative training courses for federal, state and local law enforcement agencies. Robert attained a BS and MS in Forensic Science from the University of New Haven. Additionally, Robert holds and actively maintains the following certifications: AccessData Certified Examiner (ACE), Certified Forensic Computer Examiner (CFCE), EnCase Certified Examiner (EnCE) and GIAC Certified Forensics Analyst (GCFA).